CHAPTER 2

LAN HARDWARE

Upon completing this chapter, you should be able to do the following:

- *Explain how to install, inspect, and test network components.*
- *Describe how to make physical connections to networks.*
- *Explain the function of a network server.*

As noted in chapter 1, if the hardware, network software, application software, and cabling were all supplied by the same manufacturer, we would have relatively few problems to contend with when we design and implement a network. The answers to many hardware and software incompatibilities are found in the use of interfaces. These various types of interfaces (bridges, gateways, routers, and so on) allow networks to be compatible with one another.

NETWORK COMPONENTS

More and more, LANs are becoming part of larger networks. By connecting LANs together, any peripheral device, such as external hard disk, printer, or plotter can be shared by all users of the networks. This makes more efficient use of expensive peripherals. **Repeaters** can be used to amplify electrical signals; which, in turn, allows transmissions to travel greater distances. **Bridges** (also known as bridge servers) make it possible to interconnect like LANs; that is, two similar networks. **Routers** enable networks to communicate using the most efficient path. **Brouters** combine the functions of a bridge and a router. Gateways (also known as gateway servers) make it possible to interconnect unlike LANs; that is, two dissimilar networks.

INSTALL COMPONENTS

The installation of network components is dependent on the particular type of component, the manufacturer, and the type of cable being used. When it comes to installing one of these components, read the instructions that are supplied with the component to make sure that you install it properly.

Repeaters

Repeaters are used to amplify electrical signals carried by the network. They work at layer 1 of the OSI model—the physical layer. (The OSI model was covered in chapter 1.) The function of a repeater is to receive incoming signals (a packet of data), regenerate the signals to their original strength, and retransmit them. Repeaters are used to lengthen individual network segments to form a larger extended network. That is, repeaters allow a network to be constructed that exceeds the size limit of a single physical segment by allowing additional lengths of cable to be connected (see figure 2-l). There is a catch, however. For a repeater to be used, both network segments must be identical-same network protocols for all layers, same media access control method, and the same physical transmission technique. This means we could connect two segments that use the CSMA/CD access methods, or connect two segments that are running under the

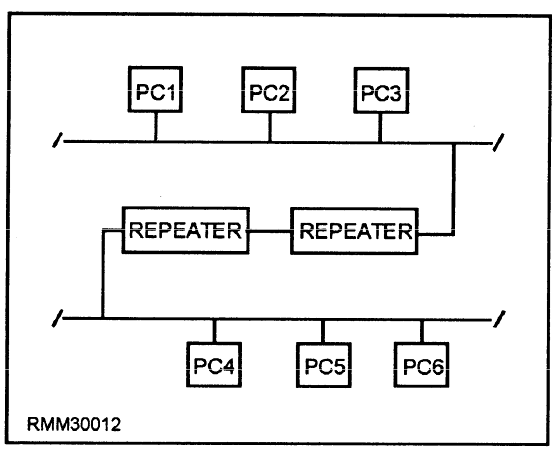

Figure 2-1.—Repeaters used to lengthen individual network segments.

token-passing access method. However, we cannot connect a CSMA/CD segment to a token-passing segment.

Bridges

Bridges handle the first two layers of the OSI model—the physical layer and the data link layer. Like repeaters, bridges connect physically-isolated networks to forma single logical network; however, a bridge has a little more intelligence and can provide some translation between dissimilar protocols. For example, our token-passing segment wants to communicate with our CSMA/CD segment. The bridge will "repackage" the message from the token-passing segment into a format that the CSMA/CD segment will understand. Then, the bridge will act as a workstation on the CSMA/CD segment and contend for access. The same thing happens in reverse. A message is sent from the CSMA/CD segment to the token-passing segment. The bridge then "repackages" the message into a format the token-passing segment is expecting and waits for the token, just like any other workstation. An important point to remember is that a bridge will pass on any message it receives. Because the bridge is not smart enough to know that unlike LANs do not understand each other, it will go ahead and send the message. Because the two LANs speak a different "language," the message will be ignored.

Routers

Routers only connect networks running similar access methods. They work at the third layer of the OSI model—the network layer. Like bridges and repeaters, routers can connect networks over different wiring media and topologies. However, unlike bridges, routers can intelligently determine the most efficient path to any destination, based on predetermined delimiters. Routers are often a better choice for interconnecting remote installations and congested networks requiring a single protocol. Let's look at this more closely.

Let's say we have a LAN made up of three token-passing segments, and each segment is connected via a bridge. For a message to go from LAN A to LAN C, it would have to travel through LAN A and LAN B before it reaches its final destination, which is LAN C. See figure 2-2, frame A. On a LAN that has large amounts of message traffic, we can see how a bridge may slow down the system. On the other hand, if the segments are separated by routers, the router on LAN A would look at the destination of the message and determine the direct route to LAN C that would be shortest route, as shown in figure 2-2, frame B.

Brouters

A brouter can work in either the second and third layers of the OSI model—the data link layer or the network layer. A brouter is a combination of a bridge and router combined. If it can't route a packet, it acts as a bridge. Brouters are particularly useful if you have two or more different networks. Working as a bridge, a brouter is protocol independent and can be used to filter local are a network traffic. Working as a router, a brouter is capable of routing packets across networks.

Gateways

Gateways work at OSI model layer 7—the application layer. A gateway functions to reconcile differences between two dissimilar networks. Messages are not only repackaged for transmission between different networks (CSMA/CD to token-passing), but the contents of the messages are converted into a format the destination can use and understand. Now our unlike LANs can talk to each other. Gateways can also provide links between microcomputer networks and mainframes.

A gateway is generally a dedicated computer with an interface card and at least some type of software for both of the environments being connected. The gateway then runs special software that provides the necessary conversion and translation services which, in turn, allow the two environments to communicate.

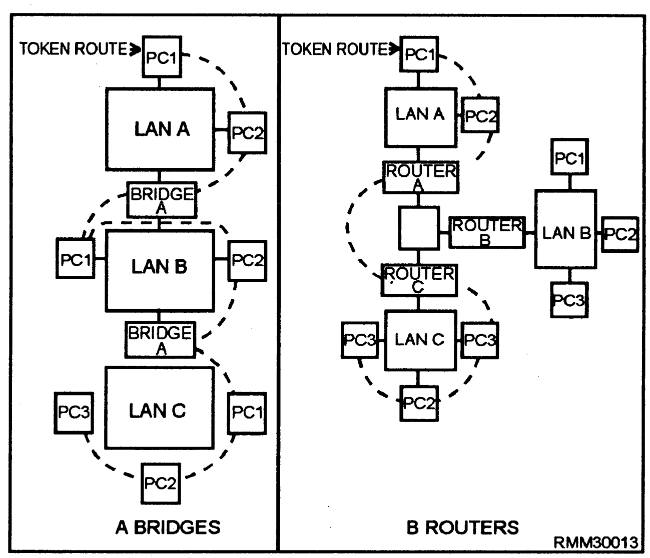

Figure 2-2.—Interconnecting LANS using (A) bridges and (B) routers.

Concentrators

The main function of a concentrator is to serve as a termination point for cable running from individual nodes in a network. The cable connects to the network or to another wire center.

A concentrator may have multiple boards or boxes mounted on a rack. Each board is essentially a hub, a wiring center for a single network's nodes. Such boards generally include light-emitting diodes (LEDs) to indicate the status of each port on the board.

Hubs

A hub is a box with a number of connectors to which multiple nodes (PCs) are attached. It serves as a common termination point that can relay signals along the appropriate paths. All hubs provide connectivity, and some even provide management capabilities. A hub usually connects nodes that have a common architecture. Although the boundary between concentrators and hubs is not always clear, hubs are generally simpler and cheaper than concentrators.

Modems

In module 2, we introduced you to modems and how they are used in a data communications environment. They translate data from digital to analog form at the sending end of the communications path and from analog to digital at the receiving end. From a conceptual standpoint, this explanation is sufficient. However, if you are going to install a modem, you need to know some of the technical aspects of modems.

MODEMS AT WORK.— Put simply, the object of a modem is to change the characteristics of a simple sine wave, referred to as a carrier signal. We know this carrier signal has several properties that can be altered to represent data. It has amplitude (height); it has frequency (a unit of time); and it has phase (a relative starting point). Modems are capable of altering one or more of these characteristics to represent data.

The job a modem performs can be divided into two discrete parts or phases at each end of the communications link. At the sending end, it converts digital bit streams (strings of 0's and 1's) into analog sine waves. This is the encoding process. Another component within the modem then changes (modulates) the analog signal so the data may be transmitted simultaneously with other data and voice traffic that has also been modulated. This process is basically reversed at the receiving end. There, the analog signal is brought back to its basic level (demodulated), and the analog sine waves are reconverted (decoded) back into their corresponding bit streams (see figure 2-3).

CODECs.— In today's digital communications lines, voice traffic is considered the outsider that digital data used to be to analog lines. Voice can enter the data communications lines only after being encoded into digital form. It then must be decoded to be audible again at the receiving end. The device used to perform the encoding and decoding functions is known as a codec. This is simply another black box conversion device that has always been in existence in a slightly different form as part of a modem.

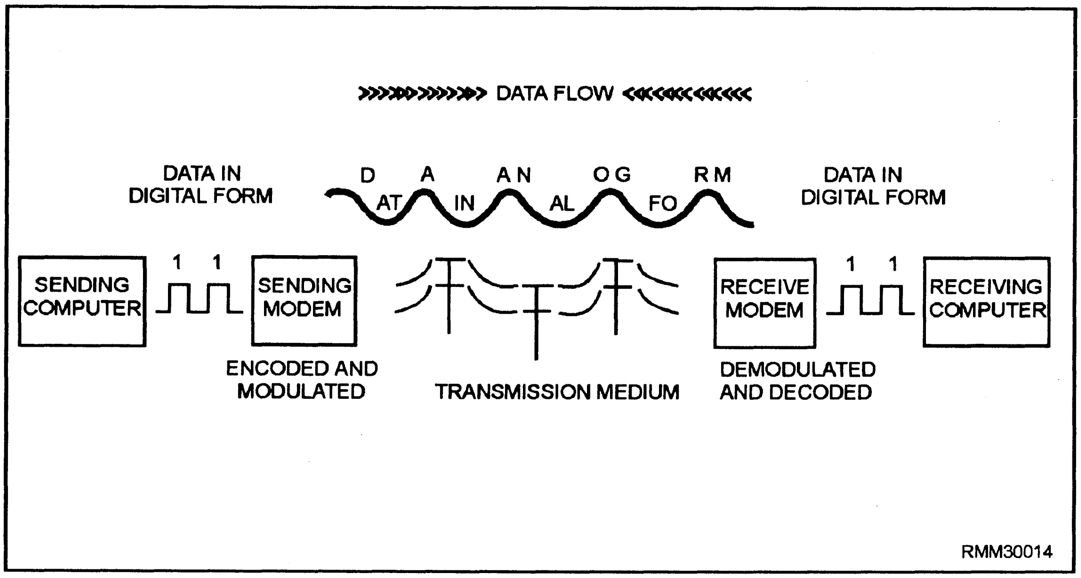

Figure 2-3.—Digital data as it is encoded, modulated, transmitted, demodulated, and decoded.

Network Interface Card and Cabling

To attach personal computers to the LAN, you must install a network interface card (NIC) into an empty expansion slot in the PC, install the appropriate software, and attach the network cable to the NIC. The other item you need to consider is what type of connector to use. But before deciding the type of connector to use, you need to know what type of cable and architecture you will be using. The cables may be twisted-pair cable, fiber optic cable, or coaxial cable.

- **Twisted-pair cable** The twisted-pair cable is easy to install and costs little on a per-foot basis. In some cases existing telephone cable may be used. Its disadvantages include limitations in capacity and speed. It is also susceptible to electrical interference unless it is shielded.

- **Fiber optic cable** Fiber optic cable is the best choice if a secure network is needed. Because the cable transmits light, the transmissions are immune to interference caused by electrical or electronic devices. Also, if your network will run through an area of heavy industrial activity or a work place with strong radio frequency interference, fiber optic cable is the most appropriate choice. Other advantages of the fiberoptic cable are that it lasts longer than other cable and can carry many more channels. Its disadvantages include its high price, poor connectivity, and low flexibility.

- **Coaxial cable** Coaxial cable, also called coax, networks have gained in popularity because of their use in cable television. The quantities of cable and connectors produced for cable television have greatly reduced the prices of these components for network users. Coaxial cable comes in various thicknesses and is designated by a number: RG-11, RG-58, RG-59, RG-62, etc. You can use either baseband or broadband transmission methods with coaxial cable.

Baseband coaxial systems, which transmit digital signals unchanged over a single channel, have several advantages. They are inexpensive, simple, easy to install, and have low maintenance. They also allow very high data transmission rates. One disadvantage is they are limited to transmitting digital signals only.

In contrast, **broadband coaxial systems** require the digital signal to be converted to an analog signal before transmission and then back to digital by modem at the receiving device. Broadband systems support data, voice, and video signals that may be transmitted simultaneously. Disadvantages of broadband systems are their higher installation costs and complex maintenance.

Connectors

The connector provides the physical link between two components. For example, a connector can link a cable and a NIC, a cable and a transceiver, or two cable segments.

Connectors differ in their shape, size, gender, connection mechanism, and function. These features influence and determine where a connector can be used. Where necessary, special adapters may be used for connections involving different connector combinations.

Connectors also differ in how sturdy they are, how easily and how often they can be attached and detached, and in how much signal loss there is at the connection point.

The type of connector needed in a particular situation depends on the components involved and, for networks, on the type of cable and architecture being used.

CONNECTOR FUNCTIONS.— A connector may be passing the signal along or absorbing it. A connector that passes a signal along may pass it unmodified or may clean and boost it. Connectors can serve a variety of purposes, including the following:

- Connect equal components, such as two segments of thin coaxial cable
- Connect almost equal components, such as thin to thick coaxial cable
- Connect unequal components, such as coaxial to twisted-pair cable
- Connect complementary components, such as a NIC to a network
- Terminate a segment

CONNECTOR SHAPES.— Specially shaped connectors are used for particular types of connections or for connections in particular locations. For example, a T-connector attaches a device to a cable segment; an elbow connector allows wiring to meet in a corner or at a wall.

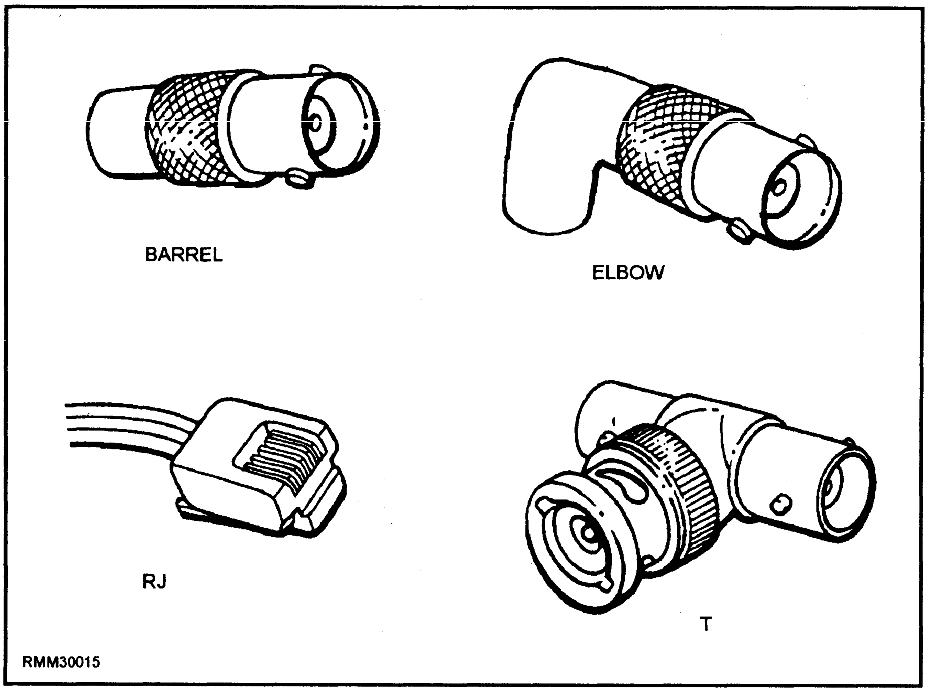

Figure 2-4.—Connector shapes.

Table 2-1.—Cable connector shapes.

SHAPE	DESCRIPTION
Barrel	Used to link two segments of cable in a straight run.
Elbow	Connector with a right-angle bend, used to connect two sections of cable in a corner or to accomplish a change of direction.
RJ	Used to connect telephones to the wall or modems.
T	Used to attach a device to a section of cable.

The connector shapes used in networking setups are listed in table 2-1. Figure 2-4 shows examples of connector shapes.

FIBER-OPTIC CONNECTORS.— Like electrical cable connectors, different types of fiber-optic connectors have different kinds of attachment mechanisms. The actual attachments between ferrule shells may be made by threading, snapping, or clicking. Table 2-2 lists the most commons types of fiber-optic connectors.

Table 2-2.—Fiber-optic connectors.

TYPE	CONNECTION METHOD	# OF MATINGS
ST (straight tip)	Barrel nut connector (BNC)	1000
SC (subscriber connector)	Pushbutton latch	1000
MIC (medium interface connector)	Pushbutton latch	1000
SMA	Threaded coupling	200

In addition to attachment mechanisms, fiber-optic connectors differ in the following ways:

- The size of the ferrule.
- Whether the connector can be keyed. This is the technique for making a connector asymmetrical, usually by adding a notch or plug, making it impossible to plug the connector in wrong.
- The number of matings the connectors can handle without producing unacceptable signal loss.

- Whether the fiber must be twisted to make the connection; multiple fibers cannot run through the same connector if it is to be twisted.

The connectors differ in the way the fiber is attached to the connector itself. You can either use epoxy to glue the fiber into the connector, or you can crimp the connector and the ferrule together using a special crimping tool.

CONNECTOR GENDERS.— Connector gender basically refers to whether a connector has plugs or sockets. The gender is important because the elements being connected must have complementary genders.

A male connector is known as a plug; the female connector is known as a jack. With a few exceptions, such as the IBM® data connectors and certain fiber-optic connectors, all connector types have distinct genders. Figure 2-5 shows examples of male and female connectors.

CONNECTOR MECHANISMS.— The connection mechanism defines how the physical contact is made to allow the signal to pass from one side of the connection to the other.

Connection mechanisms differ in how sturdy they are. For example, the pin-and-socket connection at a serial port can be wobbly without extra support from the screws on either side of the plug. On the other hand, fiber-optic connectors must be cut to precise proportions and must not allow any play in the connection.

INSPECTING COMPONENTS

The inspection of the components when they are received is limited to checking for any physical damage. This damage will include:

- Any damage to the packing material
- Damage to the case
- Hidden damage on the inside of the cabinet

The inspection that is conducted needs to be as thorough as possible, since any damage discovered must be reported to the supplier. This inspection also needs to be accomplished as soon as the equipment arrives, because the longer you wait, the less likely it becomes that the supplier will replace the equipment.

NETWORK TESTING

Network testing is changing significantly because of the growth of digital network capability. Testing in the voice network has always been considered as much of an art as a science because of the variable nature of the different impairments encountered. The digital net work has been designed with more diagnostic capability, making it much easier to identify and isolate problems. The testing is done in the carrier environment, not in the user environment.

Network Testing Methods

There are three basic approaches to network testing, as follows:

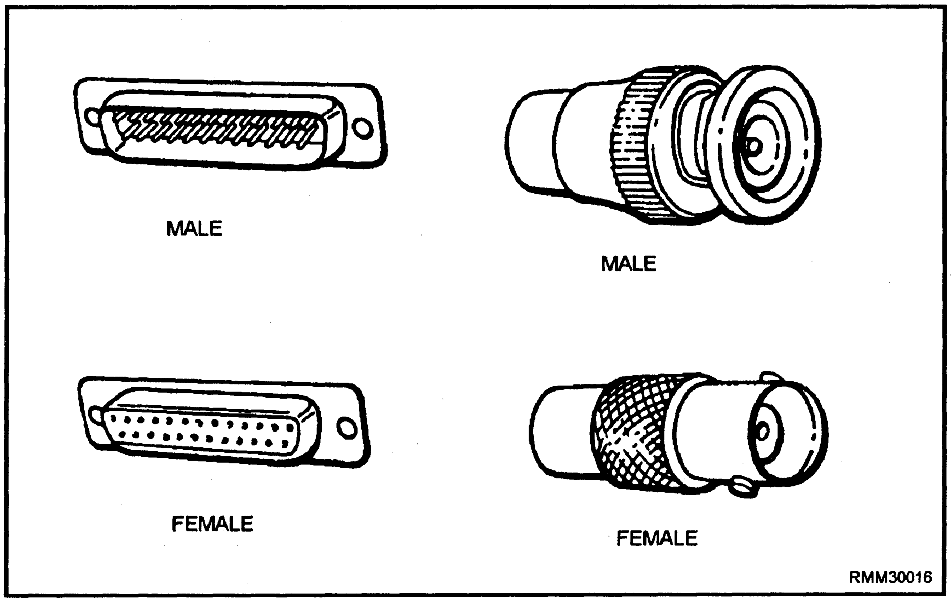

Figure 2-5.—Connector genders.

1. Rely on vendors. If you rely on a vendor for testing, you probably have a single vendor's products in your network and are, therefore, locked into that vendor. Fewer vendors today are capable of providing this complete capability.

2. Use an organization dedicated to network problem solving (third party). At one time, third-party problem solving was considered a viable alternative, but today the expertise needed is so vast and covers such a wide variety of products that it is not feasible to provide the service. The carrier providing the majority of your circuits is the best for handling your network management. However, it is difficult for the carrier to be objective, and it is usually not very cost effective.

3. Use in-house network management. In-house network control is by far the most flexible in design and operation. Network administrators typically understand their problems better than any carrier or vendor could. Network problems are not always the result of network conditions; they may actually be operational problems. A disadvantage of in-house network control is that it requires more resources, such as knowledgeable people, equipment, space, and all of the other support overhead.

Regardless of the testing method that is used, testing can be performed by both hardware tools and software programs.

Hardware Testing

The tools used are partly insurance and partly convenience devices. The greatest expense of a network comes when it is down or functioning incorrectly; it is important to be able to test components when things go wrong. Testing should also be accomplished before installing, to ensure that you do not install a faulty component. After they are installed, test components periodically to make sure they are functioning properly. Special tool are available for this purpose.

Network testers can be very expensive, while convenience tools, such as wire crimpers and voltmeters, are quite inexpensive. The amount that is spent on tools will depend on the size of the network, the importance of the network's contents, and who will be doing the maintenance on the network.

The following are several types of hardware tools:

- Manufacturing tools for creating individual components, such as crimpers and dies for attaching wires to connectors.
- Construction tools for assembling and disassembling systems; for example, screwdrivers, pliers, chip removers, and chip installers.
- Testing tools for testing individual components or for monitoring the performance of a component or system, such as voltmeters, ammeters, and line scanners.
- Safety tools for making sure components are protected against damage from electrical and other dangers; for example, static cords, electrical mats, and shorting probes.

BASIC TOOLS.— The level and range of tools you will need depends on the level of your involvement with the network. Regardless of the level, a few basic tools will almost certainly make your life easier:

- Screwdrivers, for opening machines, installing and removing expansion cards, and for attaching connectors;
- Pliers, for grasping objects;
- Wrenches or nut drivers, for tightening and loosening nuts;
- Chip removers/installers, for removing and installing computer chips; and
- Tweezers, for retrieving small parts and screws.

In addition to these tools, some people might also have wire strippers, cutters, and soldering irons that can be used to set up special-purpose circuits or wiring connectors.

If you are going to do any troubleshooting at all, you will need a voltmeter or ammeter (probably both), with an operator's manual, to test the electrical activity. Use of the manual is essential to connect the meter properly; connecting the meter wrong can cause serious damage to sensitive circuitry.

TOOLS FOR INSTALLING AND ATTACHING CABLE.— The tools used in making cables are specialized tools. They are used to attach the connectors onto the cable and then to test the cable. It is advisable to get the cables pre-made to the desired length by the manufacturer. Unfortunately, that isn't always possible.

To attach connectors to cable, you need the following tools:

- a crimping tool, for pressing the cable and connector together, and
- a die for the specified cable/connection pair, to make sure cable and connector fit properly.

Installation tool kits that include the crimping tool, die, cable, connectors, and cable ties can be purchased from manufacturers. These kits range in price from one or two hundred to several thousand dollars.

TOOLS FOR TESTING CABLES.— Voltmeters and ammeters provide readings of voltage and current, or amperage by tapping into the circuit and recording the electrical activity as it occurs. These recorded values may or may not provide the details about what is happening along the lines of the network.

Scanners are much more sophisticated testing tools. Some of the capabilities of scanners include the following:

- Check for faults in a cable.
- Test a cable's compliance with network architectures.
- Monitor performance and electrical activity, given the type of cable and architecture involved.
- Test the cable's wiring sequence.
- Generate and print a summary of the information obtained from the tests.

A powerful scanner can test for cable quality, for the quality of the connections between cable segments, or between cable and device. A less poweful scanner will be able to test for noise, crosstalk, signal attenuation, resistance, cable length, and so on.

Software Testing

Diagnostic software can be used to help anticipate or catch problems early and to help deal with the problems once they have arisen. Network versions of diagnostic software may be expensive, but they can save the system under some circumstances. For example, virus detection software can save hours of reconstruction and reloading the system. Using software to test the hard disk can identify bad disk sectors before data can be written to them and move any data from bad sectors to a safe location.

Another use of diagnostic software is performance monitoring and analysis, which involves tracking the networks behavior. This will help to identify inefficiencies and bottlenecks, so they can be elimated. While monitoring the system's performance, keep careful track of the following:

- Operating costs
- Threats to security
- User satisfaction
- User productivity

Track these areas especially during the first few weeks after the network is installed. Do not be surprised if some of these measured indicators change drastically during this period. For example, costs may drop drastically after the startup period, while user satisfaction and productivity may rise after the initial problems are resolved.

NETWORK PHYSICAL CONNECTIONS

A network connection is a linkage between network elements. Physical connections concern the cables and connectors used to create the physical layout of the network. When building a network, you must first establish the physical connections.

NETWORK BACKBONES

Backbone cable refers to the cable that forms the main trunk, or backbone, of a network. Individual nodes and other devices may be connected to this cable using special adapters and a separate stretch of cable.

Backbone cable is defined by the Electronics Industries Association/Telecommunications Industry Association-568 (EIA/TIA-568) committee as any "behind the scenes" cable; that is, cable running behind walls, in shafts, or under the ground.

The EIA/TIA-568 recognizes four types of backbone cable; they are listed in table 2-3.

The use of a backbone network to tie together a number of small access networks offers several advantages over the construction of a single large LAN. The various LANs connected to the backbone are able to operate in parallel, providing greater processing efficiency. The multiple-network approach is also more reliable, since each individual LAN can continue operating if one of the access networks, or even the backbone, fails. The backbone network must also be highly reliable, since the greater distances covered may make it difficult to locate and repair faults. The LANs that connect to the backbone must be flexible and low-cost in terms of installation and user connection.

Table 2-3.—Types of backbone cable.

Cable Type	Main	Optional
UTP	100-ohm, multipair UTP cable, to be used for voice grade communications only	
STP	150-ohm STP cable	100-ohm STP cable
Coaxial	50-ohm thick coaxial cable	75-ohm (broadband) coaxial cable
Optical Fiber	6.26/125-micron (step- or graded-index) multimode optical fiber	single-mode optical fiber

Connection to the backbone network may require a bridge, router, gateway, concentrator or hub, depending on the architectures of the various LANs and the backbone itself. The connectors used will also depend on the type of cable used for the backbone. If the backbone is coaxial cable, you would use a T-connector and barrel connectors to make the connection to another cable or a hardware device.

The backbone manages the bulk of the traffic, and it may connect several different locations, buildings, and even smaller networks. The backbone often uses a higher-speed protocol than the individual local area network (LAN) segments.

One obstacle to a successful backbone network is the high bandwidth that may be required to handle potentially heavy traffic. Because of this consideration, fiber-optic cable is the most sensible cabling for backbone networks.

NODES

The computers, or nodes, in a network may be used for workstations, servers, or both. PCs need a network interface card (NIC) installed for networking capabilities.

The NICs mediate between the computer and the network by doing the necessary processing and translation to enable users to send or receive commands and data over the network. NICs are designed to support a particular network architecture, such as Ethernet® or ARCnet®.

To connect a node directly to a backbone, you would use a drop cable for the connection. Nodes are normally connected to the backbone indirectly through a concentrator or a hub rather than with a drop cable.

The elements needed to connect a node to a network include the following:

- Cable: twisted-pair, coaxial, or fiber-optic
- Wiring centers: hubs or concentrators
- Intranetwork links: connectors, repeaters, and so on
- Internetwork links: bridges, routers, gateways, and so on

The cable provides a transmission medium, as well as the physical link between the nodes on the network. Connectors and repeaters attach cable sections to each other; connectors and transceivers attach NICs to a cable and, thereby, to the network. Transceivers enable different types of cable to be attached to each other. Terminators absorb a transmission at the end of a network, preventing the signal from traveling back in the other direction on the network. The types of intranetwork links allowed in the network depend on the type of cable used and on the network topology used.

Wiring centers serve as a focal point for network elements, and may influence the logical arrangement of nodes on the network.

Internetwork links may be bridges, routers, gateways, and soon. Such components serve to connect networks to each other. The type of internetwork link depends on whether the two networks are the same or not, and the amount of translation that is needed.

NETWORK SERVER

A server is the central computer in a network, and is responsible for managing the network. The server provides some type of network service. It may be hardware, such as a file server, or software, such as network level protocol for a transport level client.

The server provides its service to other workstations on the network or to other processes. In a server-based network, the most important hardware server is the fileserver, which controls access to the files and data stored on one or more hard disks.

A server may be dedicated or nondedicated. Dedicated servers are used only as a server, not as a workstation. Nondedicated servers are used both as a server and a workstation. Networks with a dedicated server are known as server-based networks; those with nondedicated servers are known as peer-to peer networks.

DEDICATED SERVERS

Dedicated servers cannot be used for ordinary work. In fact, access to the server is often limited to prevent any access by unauthorized users.

Most of the high-end network packages assume you are using a dedicated server. If the network has a dedicated server, it is most likely a file server.

A dedicated fileserver runs the NOS software, and workstations run smaller programs whose function is to direct user commands to the workstation's operating system or to the server. Both servers and workstations need NICs to function on the network.

NONDEDICATED SERVERS

A nondedicated server can be used as a workstation as well as a server. Using a server as a workstation has several disadvantages and is not advisable for larger networks.

The following are disadvantages of nondedicated servers as compared to dedicated servers:

- Many of the NOSs that allow the nondedicated server to run with DOS make them extremely slow and clumsy. While most dedicated servers have software that replaces DOS, such systems may also require a separate non-DOS partition on the hard disk. This allows the NOS to arrange and deal with the contents of the partition in a way that optimizes performance.
- Running applications on a DOS machine while it is also supposed to be running a network can lead to a deadly performance degradation.
- Certain tasks will tie up a DOS machine, effectively stopping the network until the task is finished.
- Adequate security is more difficult to maintain on a nondedicated server.

SUMMARY

In this chapter we discussed the different types of network components and their functions. We described cabling and the connectors used to connect the network hardware. We covered the purpose of the server and the differences between a dedicated and a nondedicated server. Remember, the driving factor for the type of hardware and cabling used is the topology of the network.